attribute or object attribute and ends with the policy class, wherein any user has any user attribute if there exists a chain of assignments that starts with the user and ends with the user attribute, wherein any object has any object attribute if there exists a chain of assignments that starts with the object and ends with the object attribute, wherein the prohibitions include user-deny relations and process-deny relations, where each user-deny relation is any triple that includes any user, any set of the operations, and any set of the objects and where each process deny relation is any triple that includes a process identifier, any set of the operations, and any set of the objects, wherein each of the obligations is any pair that includes an event pattern and a response, where the response includes a sequence of administrative operations applied to prescribed elements of the basic data sets and basic relations, and the event pattern specifies conditions that cause an event processing sub-module to execute the administrative operations on the prescribed elements when a successful execution of any operation on any object meets the conditions.

13. The general attribute-based access control method as recited in claim **12**, further comprising selectively deriving permissions from the assignments, where each permission is any triple that includes any of the users, any of the operations, and any of the objects, where for each policy class containing the object, the user has a corresponding one of the user attributes belonging to the policy class, and the object has a corresponding one of the object attributes belonging to the policy class, and there is a set of the operations that includes the operation such that the corresponding user attribute is assigned to the set of the operations and the set of the operations is assigned to the corresponding object attribute.

14. The general attribute-based access control method as recited in claim **13**, further comprising:

establishing an association between a human user and a corresponding one of the users in the basic data set using an authentication scheme such that the human user becomes an authenticated user;

establishing a session for the authenticated user, where the session includes a computer environment for the execution of the processes of the authenticated user; and

establishing whether any of the objects are accessible to the authenticated user if there is any permission that includes the user, any operation, and any of the objects.

15. The general attribute-based access control method as recited in claim **14**, including:

executing a computer program within any process attempting to perform any operation on any object included in the objects that are deemed accessible;

issuing an access request that includes the operation and the object that are subject to the execution attempt of the program to a policy enforcement sub-module;

sending the access request from the policy enforcement sub-module to an access decision sub-module;

determining in the access decision sub-module whether to grant or deny the access request using a reference mediation function that grants the access request if the triple that includes the authenticated user, the operation included in the access request, and the object included in the access request is any permission of the user and if no user-deny relation exists that is any triple including the authenticated user, any set of the operations, and any set of the objects, where the operation included in the access request is included in the set of the operations of the user-deny relation and the object included in the access request is included in the set of the objects of the user-deny relation, and if no process-deny relation exists that is any triple including the process identifier of the process, any set of the operations, and any set of the objects, where the operation included in the access request is included in the set of the operations of the process-deny relation and the object included in the access request is included in the set of the objects of the process-deny relation, otherwise the reference mediation function denies the access request;

communicating the decision to grant or deny the access request to the policy enforcement sub-module, including communicating a physical location of a resource referenced by the object included in the access request if the decision is to grant;

performing the operation included in the access request on the resource referenced by the object included in the access request and generating an event that includes the operation performed, the object, and a context including at least the user, the process identifier, and the object attributes that are assigned to the object for the decision to grant, or returning an error message to the process that issued the request if the decision is to deny; and

searching for any obligation relations with event patterns that match the event, and executing the administrative operations in response to each obligation relation, thereby dynamically modifying a database configuration.

* * * * *